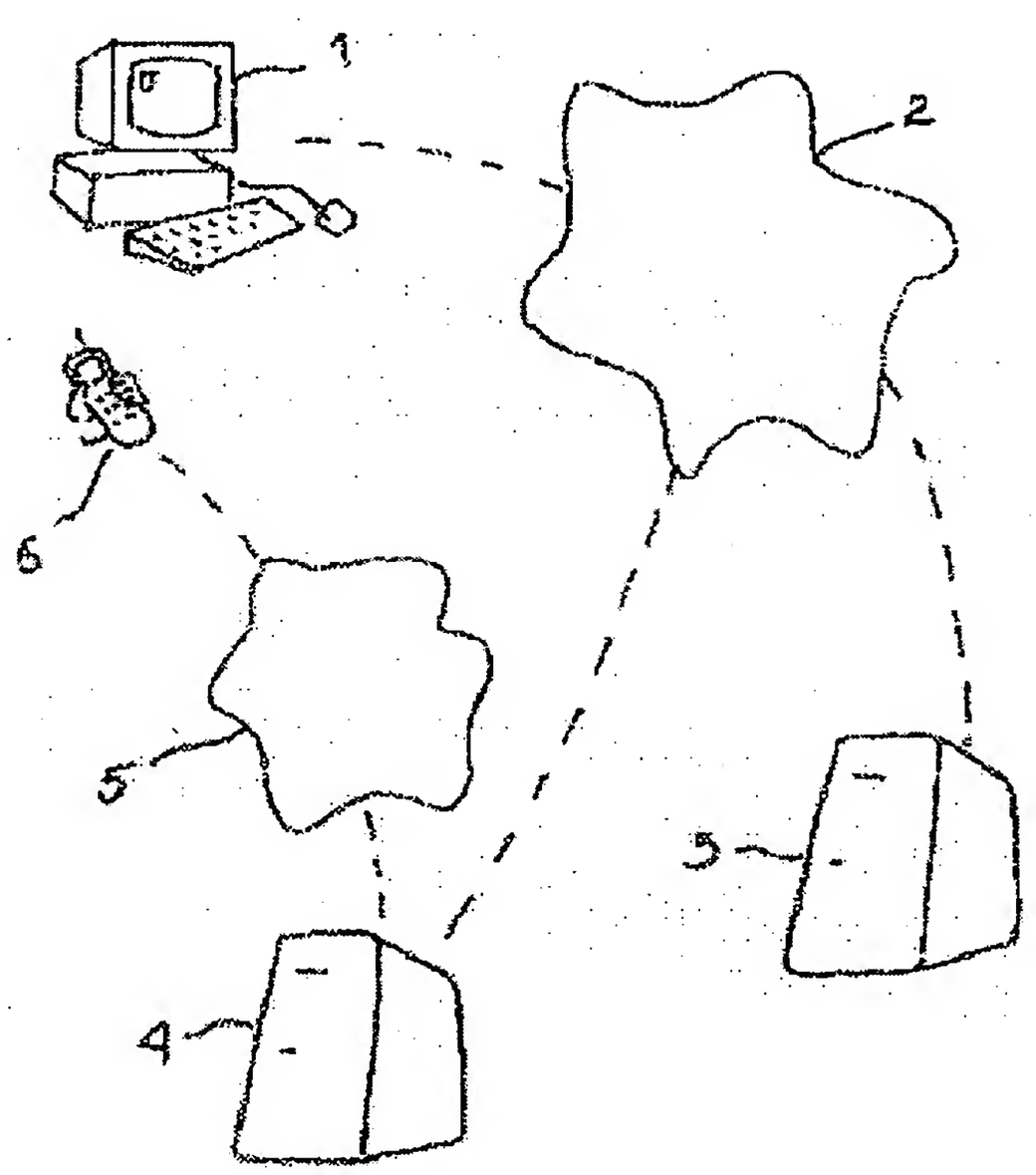
Secure communication of identification data for a limited use Internet transaction payment card, splits data into distinct packets and transmits each packet over distinct networks

Patent number: FR2828966
Publication date: 2003-02-28
Inventor: DE PANAFIEU JEAN
Applicant: SCHLUMBERGER SYSTEMS & SERVICE [FR]
Classification:
- international: H04L9/32; G06F17/60
- european: G07F19/00B
Application number: FR20010011064 20010823
Priority number(s): FR20010011064 20010823

Abstract of **FR2828966**

Each transmission and receiver (1,4,6) is designed to communicate with the other over at least two distinct telecommunication networks (2,5). The identification data is split into at least two distinct packets by the transmitter according to a data rule, then each of the packets is separately communicated by the transmitter to a distinct network. The receiver site reforms the two packets so as to reconstitute the identification data according to the data rule. The identification data consists of the card number and card expiry date. The rule forms each packet from the figures of the number and date using a pre-defined key. One of the networks is GSM or SMS cellular and the other is Internet fixed line. The transmitters/receivers are computer and mobile phone



(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** ***2 828 966***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 11064**

(51) Int Cl[7] : **H 04 L 9/32,** G 06 F 17/60

(12) **DEMANDE DE BREVET D'INVENTION** **A1**

(22) **Date de dépôt :** 23.08.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 28.02.03 Bulletin 03/09.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *SCHLUMBERGER SYSTEMES* *Société anonyme* — FR.

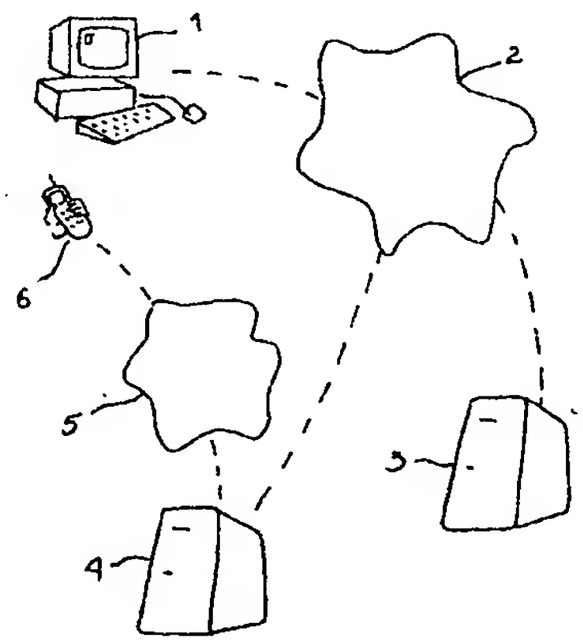
(72) **Inventeur(s) :** DE PANAFIEU JEAN.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

(54) PROCEDE POUR COMMUNIQUER DE FACON SECURISEE DES DONNEES D'IDENTIFICATION D'UNE CARTE DE PAIEMENT.

(57) Procédé pour communiquer de façon sécurisée des données d'identification d'une carte de paiement entre un site émetteur et un site récepteur, caractérisé en ce que chacun desdits sites disposant de moyens de télécommunication (1, 6, 4) aptes à communiquer avec l'autre site selon au moins deux réseaux de télécommunication distincts (2, 5), lesdites données d'identification sont réparties en au moins deux paquets distincts par le site émetteur selon une règle donnée, puis chacun des paquets est communiqué séparément par l'émetteur selon un réseau de télécommunication distinct (2, 5), le site récepteur réceptionnant des deux paquets étant alors à-même de reconstituer les données d'identification de la carte dans leur intégralité à partir de ladite règle.



FR 2 828 966 - A1

PROCEDE POUR COMMUNIQUER DE FACON SECURISEE DES DONNEES D'IDENTIFICATION D'UNE CARTE DE PAIEMENT

La présente invention concerne un procédé pour sécuriser la communication des données d'identification d'une carte de paiement.

La présente invention concerne tout particulièrement la communication des numéros de cartes temporaires encore appelées cartes de paiement à usage limité fournies par les banques à leurs clients pour sécuriser leurs transactions sur Internet.

Le terme "carte de paiement" est utilisé pour désigner toute carte bancaire à débit différé ou immédiat, toute carte de crédit, etc., émise par une banque ou un établissement spécialisé.

La sécurité des transactions effectuées au moyen de cartes de paiement repose aujourd'hui sur deux éléments : le contrôle de l'authenticité de la signature apposée par l'acheteur sur la facture, signature manuscrite ou électronique, et le contrôle de l'authenticité et de la validité de la carte en interrogeant l'établissement émetteur de la carte afin d'obtenir l'autorisation d'accepter cette carte.

Ce double contrôle est classiquement opéré par le fournisseur lorsqu'il peut disposer physiquement de la carte de paiement. La vérification de la signature manuscrite ou électronique est en effet aisée, de même pour ce qui est de la demande d'autorisation préalable. Il existe d'ailleurs des terminaux de paiement lecteurs de cartes adaptés à effectuer automatiquement de tels contrôles.

L'acheteur saisit sur le clavier d'un tel terminal, le code secret de sa carte, encore appelé PIN code (PIN étant l'acronyme anglais de Personnal Identification Number). Les circuits électroniques comparent alors le code secret saisi par l'acheteur au code inscrit de manière crypté sur la carte et ils valident la transaction en cours lorsqu'il y a coïncidence entre les deux. Par ailleurs, à partir des

informations lues sur la carte, le terminal est capable d'interroger par l'intermédiaire d'un réseau de télécommunication, un serveur de gestion des cartes de paiement qui lui confirme si la carte est bien valide et n'est pas frappée d'interdiction. Cette vérification quant à la validité de la carte pouvant se faire "on line" en appelant le serveur lors de la transaction, ou bien encore "off line" grâce au téléchargement régulier des listes de cartes interdites (listes noires ou black lists) et/ou des listes de cartes authentiques (listes positives ou white lists). Il est à noter que l'utilisation de cartes à circuits électroniques permet de contrôler directement l'authenticité de la carte.

La consultation des serveurs de gestion pour connaître le statut d'une carte de paiement et l'utilisation d'un code secret connu du seul possesseur de la carte réduisent considérablement les possibilités de fraudes.

Il n'en va toutefois plus de même, lorsque l'acheteur et le vendeur sont loin l'un de l'autre et qu'il n'est alors plus possible d'utiliser un terminal de paiement lecteur de cartes pour tester la carte

En effet, pour réaliser une transaction lorsque l'acheteur et le vendeur sont loin l'un de l'autre, par exemple lors d'un achat par correspondance, ou lors d'une réservation par téléphone ou encore lors d'une transaction électronique sur l'Internet, le vendeur se limite à demander le numéro et la date d'expiration de la carte de paiement de l'acheteur. La communication de ces seules informations suffit à valider une facture que le fournisseur présente ensuite pour encaissement à sa banque.

La simplicité du mécanisme actuel d'acquittement par carte de paiement des transactions opérées à distance est à l'origine d'un grand nombre de fraudes, puisque toute personne ayant la connaissance

d'un numéro de carte de paiement et de la date d'expiration de cette dernière peut utiliser ces informations de façon illégales pour acheter des biens ou des services et ce, tant que le véritable possesseur de la carte ne se rend pas compte des détournements dont il est victime et ne fait pas opposition auprès de l'établissement émetteur de la carte. Par ailleurs, ce système autorise des reniements abusifs de la part d'acheteurs indélicats qui refusent de voir débiter leur compte au prétexte mensonger que les transactions ont été effectuées à leur insu.

Cela est particulièrement vrai pour les transactions électroniques réalisées sur l'Internet puisque, sur un tel réseau de communication ouvert, il est particulièrement facile d'intercepter les informations qui y sont échangées. Cette insécurité est aujourd'hui un frein important au commerce sur l'Internet.

De nombreuses tentatives ont été lancées pour pallier cet inconvénient et rendre les transactions à distance plus sûres et notamment les transactions électroniques.

Parmi ces tentatives on peut citer les systèmes du type SET qui consistent à crypter les informations échangées sur Internet. Avec de tels systèmes les numéros de cartes bancaires ne sont donc plus communiqués ouvertement et ne sont donc plus interceptables. La mise en œuvre de tels systèmes butte toutefois sur la mise à disposition du plus grand nombre, des moyens spécifiquement prévus pour sécuriser les transactions comme des lecteurs de cartes pour ordinateurs, des moyens de chiffrage dans les ordinateurs ou dans les lecteurs, et la standardisation des protocoles choisis par les différents opérateurs. Par ailleurs, si les numéros ne sont plus directement interceptables lors de la communication entre l'acheteur et le site Web, ils peuvent toujours l'être sur le site Web où les numéros de carte se retrouvent stockés sous une forme décryptée et ils peuvent l'être sur

l'ordinateur du titulaire à partir de programmes espions résidents adaptés à enregistrer les informations saisies par le titulaire sur les touches de son ordinateur.

Une autre approche, consiste à utiliser une carte de paiement temporaire ou à usage limité. Une telle carte est généralement créée par l'établissement financier de l'acheteur, à la demande de ce dernier. Cette carte dont la durée de vie est généralement limitée à une transaction ou encore à une somme donnée d'argent, se présente essentiellement sous la forme d'un numéro et d'une date d'expiration ayant les mêmes formats ISO que la carte de paiement principale de l'acheteur (de type Visa, Mastercard, etc.).

Cette solution nécessite donc la transmission de manière sécurisée des numéros des cartes temporaires aux acheteurs. La solution généralement choisie par les banques consiste à utiliser des liaisons cryptées de type SSL entre les ordinateurs des acheteurs et les serveurs bancaires. Cette méthode n'est toutefois pas sans risque de fraude puisque les méthodes développées par les fraudeurs sur Internet deviennent de plus en plus performantes.

L'objet de la présente invention est donc de proposer une alternative pour transmettre de façon confidentielle aux usagers les données d'identification des cartes temporaires, tels que les numéros et les dates d'expiration, alternative qui soit toute à la fois sûre et simple à mettre en oeuvre.

Le procédé selon l'invention a donc pour objet de communiquer de façon sécurisée des données d'identification d'une carte de paiement entre un site émetteur et un site récepteur.

Selon l'invention, ce procédé est caractérisé en ce que chacun desdits sites disposant de moyens de télécommunication aptes à communiquer avec l'autre site selon au moins deux réseaux de

télécommunication distincts, lesdites données d'identification sont réparties en au moins deux paquets distincts par le site émetteur selon une règle donnée, puis chacun des paquets est communiqué séparément par l'émetteur selon un réseau de télécommunication distinct, le site récepteur réceptionnant des deux paquets étant alors à-même de reconstituer les données d'identification de la carte dans leur intégralité à partir de ladite règle.

Selon une autre caractéristique du procédé objet de la présente invention, les données d'identification consistent dans le numéro et la date d'expiration de ladite carte.

Selon une autre caractéristique du procédé objet de la présente invention, la règle consiste à former chaque paquet à partir des chiffres du numéro et de la date répartis selon une clé prédéfinie.

Selon une autre caractéristique du procédé objet de la présente invention, l'un des réseaux de télécommunication est un réseau téléphonique.

Selon une autre caractéristique du procédé objet de la présente invention, l'un des réseaux de télécommunication est un réseau téléphonique cellulaire de type GSM.

Selon une autre caractéristique du procédé objet de la présente invention, le paquet de données transitant par ledit réseau de téléphonie cellulaire est transmis sous forme d'un message SMS.

Selon une autre caractéristique du procédé objet de la présente invention, l'un des réseaux de télécommunication est l'Internet.

Selon une autre caractéristique du procédé objet de la présente invention, le paquet de données transitant par ledit réseau Internet est transmis sous forme chiffrée.

Selon une autre caractéristique du procédé objet de la présente invention, les deux sites sont formés respectivement d'un usager

disposant de moyens d'émission/réception appropriés et d'un serveur bancaire à distance.

Selon une autre caractéristique du procédé objet de la présente invention, lesdits moyens à la disposition de l'usager sont formés d'un micro-ordinateur équipé d'un modem et d'un téléphone mobile.

On comprendra mieux les buts, aspects et avantages de la présente invention, d'après la description donnée ci-après de plusieurs modes de réalisation de l'invention, présentés à titre d'exemples non limitatifs, en se référant au dessin annexé, dans lequel :

la figure 1 est une vue schématique du système nécessaire à la mise en œuvre du procédé selon la présente invention.

En se reportant à la figure 1, seuls les éléments utiles à la compréhension de l'invention, ont été figurés.

L'exemple qui a été choisi pour illustrer le procédé et son dispositif de mise en œuvre selon l'invention, concernent l'utilisation d'une carte de paiement temporaire pour opérer une transaction électronique sur le réseau Internet. Bien évidemment, l'invention n'est pas limitée à ce seul exemple et concerne plus généralement la communication sécurisée des données d'identification d'une carte de paiement, tels que son numéro, sa date de validité ou encore un PIN code, cette communication s'opérant entre deux sites distants et notamment entre le domicile d'un usager et son établissement financier.

Selon la représentation de la figure 1, le système nécessaire à la mise en œuvre de l'invention est le suivant. Un acheteur est installé devant un ordinateur qui est par exemple son micro-ordinateur personnel référencé 1, lequel est équipé d'un modem permettant sa connexion au réseau Internet 2. L'ordinateur 1 est connectable via le réseau Internet 2 au serveur 3 d'un site marchand proposant un

service de vente de bien ou de service comme par exemple un service de vente de livres. L'ordinateur 1 est également connectable via le réseau Internet 2 au serveur de gestion 4 de son établissement financier. La liaison entre le serveur de gestion 4 et le micro-ordinateur de l'acheteur est de préférence sécurisée étant par exemple de type SSL.

L'acheteur dispose par ailleurs d'un téléphone mobile 6 muni d'une carte SIM (Subscriber Identity Module). Ce téléphone 6 est apte à recevoir ou à émettre à travers un réseau 5 de radio télécommunication de type GSM ou autre, des données en provenance ou à destination du serveur 4 sous la forme de messages radioélectriques émis selon un protocole dit de service de message court, aussi connu sous le nom de SMS (Short Message Service). Ce protocole autorise des messages d'une longueur de 160 caractères. On peut chaîner jusqu'à quinze messages consécutifs, soit 2400 caractères dans un message. De plus ce protocole est présent sur tous les téléphones mobiles du marché. Il est en général utilisé par les opérateurs par exemple pour prévenir leurs abonnés qu'ils ont reçu de nouveaux messages dans leurs boîtes vocales.

L'acheteur s'étant connecté au site marchand 3 à travers le réseau Internet 2 au site marchand 3 et ayant choisi d'acheter un livre il reçoit du site 3 un formulaire d'enregistrement de sa commande où doivent être saisies un certain nombre d'informations, tels que le numéro et la date d'expiration d'une carte de paiement. Dans la mesure où l'acheteur ne souhaite pas communiquer ouvertement les informations relatives à sa propre carte de paiement, celui-ci va utiliser en lieu et place une carte temporaire obtenue auprès de sa banque. Pour ce faire, l'acheteur va donc ouvrir en parallèle une

seconde session de connexion via un logiciel approprié et se connecter via le réseau Internet 2 au serveur 4 de son établissement financier.

L'objet de la connexion au serveur de gestion 4 est d'obtenir une carte de paiement temporaire qui ne sera valable que pour une seule transaction.

Ces cartes de paiement temporaires sont parfaitement similaires quant aux prestations offertes à la carte permanente de l'acheteur. Elles sont associées au même compte bancaire et peuvent être acceptées par les mêmes commerçants que la carte permanente (réseaux Visa, Mastercard, etc.). Leurs principales différences résident dans le fait qu'elles ne sont valables que pour un nombre limité de transactions et de préférence que pour une seule transaction. De préférence, ces cartes ont de plus une durée de vie relativement brève de quelques dizaines de secondes à quelques jours.

Bien que pouvant être utilisées pour toute transaction commerciale, ces cartes temporaires de paiement sont particulièrement adaptées pour les transactions à distance. Les cartes temporaires de paiement peuvent en particulier ne pas avoir de support physique (affichage temporaire sur un écran ou encore communication verbale).

Hormis ces différences, les cartes temporaires de paiement sont parfaitement similaires aux autres cartes notamment quant au format et au codage de leurs numéros ou à leur date d'expiration (format à quatre chiffres : mois/année (07/01)). Ainsi, dans la mesure où les cartes de paiement traditionnelles comportent des numéros à seize chiffres, alors chaque numéro de carte temporaire comporte aussi seize chiffres : les six premiers chiffres formant le code BIN de l'organisme financier émetteur et le dernier chiffre le code d'authentification de Luhn (CHECKSUM). Bien évidemment le format à

seize chiffres n'est pas limitatif de l'invention, les numéros des cartes temporaires pouvant prendre n'importe quelle autre forme : série de dix-neuf chiffres, série alphanumérique de longueur donnée, etc.

Il est par ailleurs possible de fournir à chaque carte temporaire, un code secret encore appelé PIN code (Personal Identification Number). La carte temporaire peut comporter également de façon plus précise sa date et son heure de fin de validité (par exemple au format jour/mois/année heure (27/07/01 14:31)), cette information est destinée au seul titulaire de la carte.

L'acheteur demande donc la création d'une carte temporaire de paiement au serveur de gestion 4 afin de saisir les données de cette carte dans les champs correspondants du formulaire de commande présenté par le site marchand 3.

Conformément à l'invention, le serveur de gestion 4 communique alors les données d'identification de la carte temporaire de paiement demandée à l'acheteur selon le procédé sécurisé suivant.

Pour la suite de la description de l'invention nous considérerons que la carte temporaire allouée par le serveur de gestion à l'acheteur suite à sa requête, a le numéro 4524 6434 3211 4635 (ce numéro est donné à titre d'exemple d'un numéro à 16 chiffres et ne comporte donc pas à priori de code BIN et de code CHECKSUM valables) et la date d'expiration 0701. Les données d'identification de la carte temporaire sont alors décomposées automatiquement par le serveur de gestion 4 selon au moins deux paquets de données. Le premier paquet « 4524643432 » est par exemple formé des 10 premiers chiffres du numéro de la carte et le second paquet « 1146350701 » formé des 6 derniers chiffres du numéro auxquels est accolée la date d'expiration.

Bien évidemment ce partage en deux paquets de même dimension n'a été donné qu'à titre d'exemple et toute autre décomposition est

couverte par la présente invention. Ainsi le premier paquet pourrait contenir quatorze chiffres et le second six, ou bien encore le premier sept chiffres et le second treize, etc. De même la décomposition des données d'identification peut se faire en plus de deux paquets, par exemple en trois ou en quatre, etc.

De même la composition des paquets peut être plus élaborée. Ainsi chaque paquet pourrait être formé à partir des chiffres du numéro et de la date d'expiration selon une clé de répartition prédéfinie, etc.

Les paquets de données ainsi formés sont ensuite envoyés à l'acheteur via des canaux de communication différents. Le premier paquet est par exemple transféré via le réseau Internet 2 et la liaison SSL et apparaît alors sur l'écran du micro-ordinateur 1 de l'acheteur. Le second paquet est envoyé quant à lui via le réseau de radio télécommunication 5 sous la forme d'un SMS qui vient alors se stocker dans les mémoires correspondantes du téléphone mobile 6 de l'acheteur. Seul l'acheteur est alors de reconstituer les données complètes de la carte de paiement temporaire en combinant les deux paquets d'informations reçus selon les deux canaux.

L'acheteur n'a donc plus alors qu'à rentrer le numéro reconstitué et la date d'expiration dans le formulaire de commande du site marchand 3.

Etant donné, que le numéro et la date d'expiration saisis par le titulaire sont parfaitement similaires à ceux d'une carte de paiement traditionnelle, le marchand n'a pas à modifier ses procédures transactionnelles pour accepter la commande du titulaire payée au moyen de la carte temporaire. Le marchand n'a d'ailleurs aucune possibilité de différencier les numéros et donc la nature des cartes de paiement qui lui sont communiquées.

Le marchand procède donc à une demande d'autorisation de façon tout à fait classique. Ayant obtenue en retour l'autorisation demandée, la transaction est validée et le livre commandé peut être livré à l'acheteur. Le marchand n'a plus alors qu'à remettre la facture correspondante à son établissement financier pour que ce dernier puisse obtenir de l'établissement émetteur le transfert des fonds.

La transmission du numéro de paiement temporaire se trouve ainsi parfaitement sécurisée. Le fractionnement des données d'identification de la carte, une partie via le micro-ordinateur et une partie via le téléphone mobile, permet de sécuriser l'envoi d'une carte de paiement temporaire et ce, à peu de frais puisque l'acheteur en ligne est presque toujours aussi équipé d'un GSM. La complexité de la procédure demandée au client est relativement réduite. Elle permet même de simplifier l'accès à la carte de paiement temporaire en permettant de mettre l'accent seulement sur la partie du numéro envoyée sous de forme de SMS reçu sur téléphone mobile.

La sécurité offerte par cette double transmission selon deux réseaux distincts est très grande puisque pour qu'un tiers puisse connaître la totalité des données d'identification de la carte de paiement de l'acheteur, il faut qu'il soit capable de capter la communication téléphonique du serveur de gestion 4 vers le téléphone 6 de l'acheteur et qu'il est également eu accès à la session de connexion Internet de l'acheteur au même serveur de gestion.

Le tiers souhaitant espionner le numéro de la carte de paiement envoyé par la banque à son client, doit donc non seulement surveiller la ligne téléphonique de ce dernier mais encore enregistrer l'ensemble des différentes pages écrans affichées sur l'écran d'ordinateur du client. Il s'agit là d'un travail qui suppose des capacités de surveillance hors de portée des traditionnels fraudeurs.

L'utilisation combinée d'Internet et des réseaux de télécommunication téléphoniques pour communiquer les données des cartes temporaires de paiement permet d'obtenir ces dernières en permanence, 24 heures sur 24 heures, quelle que soit la localisation géographique de l'utilisateur.

Bien évidement l'invention n'est pas limitée à ce mode de réalisation.

Ainsi la partie des données communiquée téléphoniquement pourrait l'être non pas à travers un réseau de radio télécommunication de type GSM ou autre, mais à travers le réseau téléphonique public commuté PSTN (Public Switching Telephone Network).

Ainsi l'invention concerne plus généralement l'envoi des données d'identification d'une carte de paiement, qu'elle soit temporaire ou non, entre deux sites. Elle s'applique ainsi à la situation où un client doit fournir les références de sa carte à un fournisseur de services. Ainsi considérons un client devant s'enregistrer auprès d'un opérateur de télécommunication gestionnaire d'un service de paiement sécurisé à partir d'un PC ou d'un mobile. Lors de l'inscription du client au service, le client doit communiquer à l'opérateur son numéro de carte réelle. Cette communication est alors opérée pour partie à partir de son PC et le reste à partir de son mobile, bénéficiant ainsi de la sécurité de 2 réseaux indépendants: Internet et GSM.

Bien évidemment, l'accès aux données transmises par le serveur de gestion 4 relatives à la carte de paiement tant via le réseau Internet que via le réseau téléphonique peut être soumis à l'identification et à l'authentification préalable de l'acheteur au moyen de mot(s) de passe approprié(s).

Ainsi les données d'identification des cartes de paiement transmises par voie téléphonique peuvent l'être de différentes

manières et non seulement par SMS. Ainsi elles peuvent l'être vocalement (énonciation verbale sur la ligne), en clair ou de façon codée en utilisant par exemple une clé de cryptage de type Jules César, où à chaque chiffre de zéro à neuf est associé une lettre, la clé de cryptage ayant été donné préalablement et de façon sécurisée par l'établissement financier à l'utilisateur.

REVENDICATIONS

1/ Procédé pour communiquer de façon sécurisée des données d'identification d'une carte de paiement entre un site émetteur et un site récepteur, caractérisé en ce que chacun desdits sites disposant de moyens de télécommunication (1,6,4) aptes à communiquer avec l'autre site selon au moins deux réseaux de télécommunication distincts (2,5), lesdites données d'identification sont réparties en au moins deux paquets distincts par le site émetteur selon une règle donnée, puis chacun des paquets est communiqué séparément par l'émetteur selon un réseau de télécommunication distinct (2,5), le site récepteur réceptionnant des deux paquets étant alors à-même de reconstituer les données d'identification de la carte dans leur intégralité à partir de ladite règle.

2/ Procédé selon la revendication 1, caractérisé en ce que lesdites données d'identification consistent dans le numéro et la date d'expiration de ladite carte.

3/ Procédé selon la revendication 2, caractérisé en ce que ladite règle consiste à former chaque paquet à partir des chiffres du numéro et de la date répartis selon une clé prédéfinie.

4/ Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'un des réseaux de télécommunication est un réseau téléphonique (5).

5/ Procédé selon la revendication 4, caractérisé en ce que l'un des réseaux de télécommunication est un réseau téléphonique cellulaire de type GSM (5).

6/ Procédé selon la revendication 5, caractérisé en ce que le paquet de données transitant par ledit réseau de téléphonie cellulaire (5) est transmis sous forme d'un message SMS.

7/ Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'un des réseaux de télécommunication est l'Internet (2).

8/ Procédé selon la revendication 7, caractérisé en ce que le paquet de données transitant par ledit réseau Internet (2) est transmis sous forme chiffrée.

9/ Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdits sites sont formés respectivement d'un usager disposant de moyens d'émission/réception appropriés et d'un serveur bancaire à distance.

10/ Procédé selon la revendication 9, caractérisé en ce que lesdits moyens sont formés d'un micro-ordinateur équipé d'un modem (1) et d'un téléphone mobile (6).

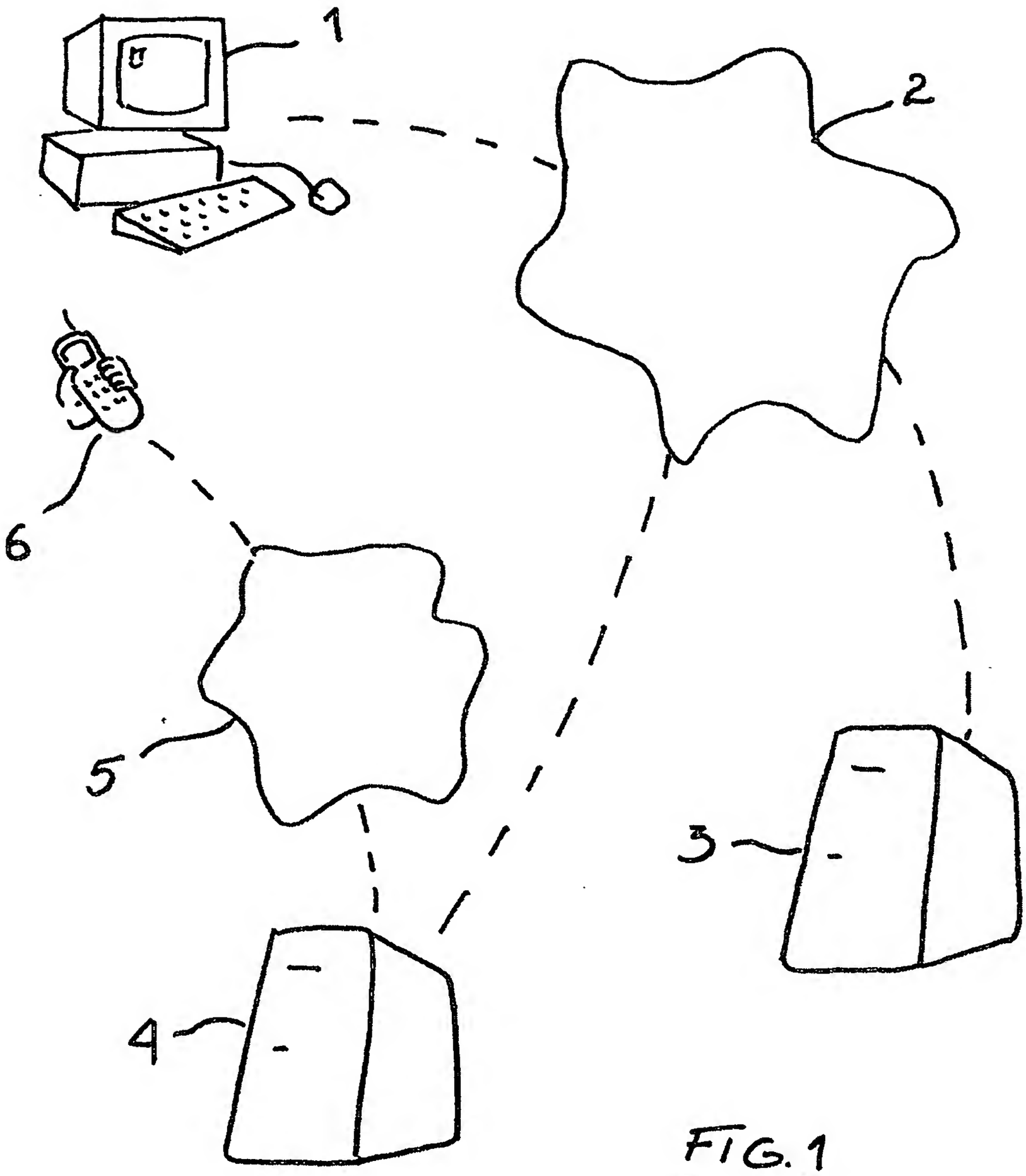


FIG. 1